Perancangan Aplikasi Pengamanan Pesan Menggunakan Algoritma Elgamal Berbasis Android

Triani Arista[1], Murdani[2]

[1,2]STMIK Budi Darma, Jl.Sisingamangaraja No.338 Simpang Limun Medan, Indonesia

ARTICLE INFORMATION

Received: Februari, 20, 2020
Revised: Maret, 6, 2020
Available online: April,9 2020

KEYWORDS

Kriptografi, Algoritma ELGamal, Android

CORRESPONDENCE

Phone: +6285297505332

E-mail: murdanimkom@gmail.com

A B S T R A K

Penyadapan data yang disampaikan saat berkomunikasi tentunya menjadi masalah apabila data yang disampaikan tersebut bersifat rahasia. Untuk itu dibutuhkan sistem pengamanan data, ketika data tersebut disampaikan kepihak yang bersangkutan maka kecil kemungkinan untuk disadap oleh pihak yang tidak berwenang. Algoritma Elgamal merupakan salah satu algoritma kriptografi kunci-publik yang dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada umumnya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan deskripsi. ElGamal digunakan dalam perangkat lunak sekuriti yang dikembangkan oleh GNU, program PGP, dan pada sistem sekuriti lainnya. Kekuatan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Dalam penelitian ini dibahas tentang cara mengamankan pesan berbasis mobile android dengan algoritma elgamal. Aplikasi dibangun dengan bahasa pemrograman java dan eclipse galileo sebagai edi kode program.tor untuk mengedit.

PENDAHULUAN

Tidak semua hal yang dikomunikasikan bersifat umum sehingga bisa dikethui oleh banyak orang. Ada kalanya hal yang dikomunikasikan tersebut bersifat private atau rahasia sehingga hanya orang-orang tertentu yang bisa mengetahuinya. Terjadi penyadapan terhadap pesan yang disampaikan saat komunikasi, tentunya menjadi masalah apabila pesan tersebut bersifat rahasia [1].

Untuk itu dibutuhkan pengamanan pesan, ketika pesan tersebut disampaikan ke pihak yang bersangkutan, pesan yang dikirim melalui media tersebut belum tentu terjamin keamanannya karena media yang menghubungkan antara pengirim dan penerima. Jika ingin informasi/pesan aman dari pengirim ke penerima maka sebaiknya terlebih dahulu merubah informasinya menjadi kode/isyarat atau ekripsi dan nanti setelah sampai ke penerima untuk membaca pesan asli terlebih dahulu melakukan dekripsi [2], [3]. Kode inilah yang akan dimanipuasi dengan berbagai macam cara untuk diubah kembali menjadi pesan kepada sipenerima. Maka dimungkinkan bisa terjadi pencurian dan pengubahan pesan yang dilakukan oleh penyadap atau cracker untuk kemungkinan tertentu

Beberapa rumusan masalah yang diambil dari latar belakang di atas adalah: Bagaimana merancang aplikasi pesan dengan menerapkan algoritma ELGamal dalam pengamanan pesan serta bagaimana menerapkan aplikasi pesan pada handphone berbasis android. Sedangkan batasan masalah adalah Aplikasi hanya untuk dua pengguna (client dan server), Pesan yang digunakan hanya pesan text. dan Bahasa pemrograman yang digunakan adalah Android Gingerbread 2.3.

LANDASAN TEORI

2.1 Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yangmempelajari teknik-teknik matematika yang berhubungan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data[2], [4]. Secara umum kriptografi adalah ilmu dana seni untuk menjaga kerahasiaan berita *(bruce Schneire-Applied Cryptography)*.

Selain defenisi tersebut ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi [4]

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keaamanan informasi yaitu :

1. Kerahasiaan, adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak
2. Integritas data, adalah layanan yang menjamin pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi, adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-phak yang berkomunikasi *(user authentication* atau *entry authentication)* maupun mengidentifikasi kebenaran sumber pesan (*origin authentication*).
4. Nirpenyangkalan *(non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerimaan pesan menyangkal telah menerimanya[4], [5].

2.2 Algoritma Elgamal

Algoritma Elgamal merupakan salah satu algoritma kriptografi kunci-publik yang dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada umumnya digunakan untuk digital signature, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk

enkripsi dan deskripsi. ElGamal digunakan dalam perangkat lunak sekuriti yang dikembangkan oleh GNU, program PGP, dan pada sistem sekuriti lainnya. Kekuatan algoritma ini terletak pada sulitnya menghitung logaritma diskrit [6].

Algoritma Elgamal tidak dipatenkan. Tetapi, algoritma ini didasarkan pada algoritma Diffie – Hellman, sehingga hak paten algoritma Diffie – Hellman juga mencakup algoritma ElGamal. Karena hak paten algoritma Diffie – Hellman berakhir pada bulan April 1997, maka algoritma ElGamal dapat diimplementasikan untuk aplikasi komersil.
Besaran-besaran yang digunakan di dalam algoritma ElGamal[7]:
1. Bilangan prima, p (tidak rahasia)
2. Bilangan acak, g (g < p) (tidak rahasia)
3. Bilangan acak, x (x < p) (rahasia)
4. M (plainteks) (rahasia)
5. a dan b (cipherteks) (tidak rahasia)

Algoritma pembangkit kunci pada sistem kriptografi ELGamal terdiri dari tiga prosedur[8]:
1. Pilih sembarang bilangan prima p besar sebagai basis group perkalian (Z*P,X)
2. Pilih dua buah bilangan acak, g dan x, dengan syarat g < p dan 1 = x = p – 2
3. Hitung β = αd mod p.

Kpublik = (ρ,α,β), Kprivate = d

Algoritma enkripsi sistem kriptografi ELGamal mengembalikan teks sandi yang terdiri sari 2 nilai: e1 dan e2. Teks asli P harus menghilangkan integer anggota Z*P.
1. Plainteks disusun menjadi blok-blok m1, m2, …, sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai p – 1.
2. Pilih bilangan acak k, yang dalam hal ini 0 £ k £ p – 1, sedemikian sehingga k relatif prima dengan p – 1.
3. Setiap blok m dienkripsi dengan rumus
   a = gk mod p
   b = ykm mod p
   Pasangan a dan b adalah cipherteks untuk blok pesan m. Jadi, ukuran cipherteks dua kali ukuran plainteksnya.
   (Sumber: Rifki Sadikin, 2012, 275)

Algoritma enkripsi sistem kriptografi ELGamal menerima teks sandi C1 dan C2 dan menggunakan kunci private d dapat Memulihkan teks asli P. (Rifki Sadikin, 2012, 277)..

HASIL DAN PEMBAHASAN

Pesan adalah setiap pemberitahuan, kata, atau komunikasi baik lisan maupun tertulis, yang dikirimkan dari satu orang ke orang lain. Pada algoritma Elgamal mempunyai panjang maksimal penentuan bilangan prima adalah P = 257, langkah selanjutnya melakukan analisis enkripsi pesan pada Algoritma Elgamal yang bertujuan untuk merubah pesan asli (plaintext) ke bentuk pesan rahasia (ciphertext). Adapun urutan proses pesan tersebut adalah :

1. Masukan teks yang akan dienkripsi *(Plaintext)*
   Plaintext = **"T R I A N I "**
2. Pesan akan dipotong menjadi blok – blok karakter dan dikonversikan ke dalam bilangan ASCII.

Tabel 1 Konversi Blok karakter ke dalam kode ASCII

I	Karakter	Plainteks MI	Plainteks mi ASCII
1	T	m1	84
2	R	m2	82
3	I	m3	73
4	A	m4	65
5	N	m5	78
6	I	m6	73

Langkah selanjutnya, Proses menentukan bilangan acak $P \in \{0,1, \ldots \ldots \ldots .. 257\}$ kemudian nilai ASCII tersebut dimasukkan ke dalam blok-blok nilai m secara berurutan, sehingga menjadi :

Mn	**Nilai**	**Kunci**
m1	84	27

m2	82	105
m3	73	13
m4	65	117
m5	78	23
m6	73	90

kemudian dihitung $y \equiv g^x \ mod\ p$ dan $m1 \equiv b1.a1^{p-1-x} \ mod\ p$
Misalkan Acak membangkitkan pasangan kunci dengan memilih bilangan:
p = 257
g = 17
x = 11
Kemudian p, g, x digunakan untuk menghitung y :

$$y \equiv g^x \ mod\ p$$
$$y \equiv 17^{11} \ mod\ 257$$
$$\boldsymbol{y \equiv 223}$$

Hasil algoritma ini adalah :
kunci publik adalah triple (223, 17, 257)
kunci private adalah pasangan (11, 257)
dimana Enkripsi a adalah :

$$\boldsymbol{a \equiv g^k \ mod\ p}$$
$$\boldsymbol{a1 \equiv 17^{27} \ mod\ 257}$$
$$\boldsymbol{a1 \equiv 34}$$
$$\boldsymbol{a2 \equiv 17^{105} \ mod\ 257}$$
$$\boldsymbol{a2 \equiv 15}$$
$$\boldsymbol{a3 \equiv 17^{13} \ mod\ 257}$$
$$\boldsymbol{a3 \equiv 197}$$
$$\boldsymbol{a4 \equiv 17^{117} \ mod\ 257}$$
$$\boldsymbol{a4 \equiv 68}$$
$$\boldsymbol{a5 \equiv 17^{23} \ mod\ 257}$$
$$\boldsymbol{a5 \equiv 120}$$
$$\boldsymbol{a6 \equiv 17^{90} \ mod\ 257}$$
$$\boldsymbol{a6 \equiv 2}$$

dimana Enkripsi b adalah :

$$\boldsymbol{b \equiv y^k\, m\ mod\ p}$$
$$\boldsymbol{b1 \equiv 223^{27}\ 84\ mod\ 257}$$
$$\boldsymbol{b1 \equiv 232}$$
$$\boldsymbol{b2 \equiv 223^{105}\ 82\ mod\ 257}$$
$$\boldsymbol{b2 \equiv 147}$$
$$\boldsymbol{b3 \equiv 223^{13}\ 73\ mod\ 257}$$
$$\boldsymbol{b3 \equiv 162}$$
$$\boldsymbol{b4 \equiv 223^{117}\ 65\ mod\ 257}$$
$$\boldsymbol{b4 \equiv 167}$$
$$\boldsymbol{b5 \equiv 223^{23}\ 78\ mod\ 257}$$
$$\boldsymbol{b5 \equiv 54}$$
$$\boldsymbol{b6 \equiv 223^{90}\ 73\ mod\ 257}$$
$$\boldsymbol{b6 \equiv 187}$$

Setelah mendapatkan nilai enkriipsi a dan b, hasil perhitungan tersebut disusun dengan cara selang seling a1, b1, a2, b2, a3, b3, a4, b4, a5, b5, a6, b6.

Sehingga membentuk chiperteks :
34, 232, 15, 147, 197, 162, 68, 167, 120, 54, 2, 187.
Di dalam bentuk karakter menjadi : "éSIˇÅ¢D§X6SOH››

Cipherteks akan di potong menjadi blok – blok karakter dan di konversikan ke dalam bilangan ASCII.

Tabel 2 Konversi Blok Cipherteks ke dalam kode ASCII

I	Karakter	Planiteks Mi	Plainteks mi (ASCII)
1	"	M_1	34
2	é	M_2	232
3	SI	M_3	15
4	□	M_4	147
5	Å	M_5	197
6	¢	M_6	162
7	D	M_7	68
8	§	M_8	167
9	X	M_9	120
10	6	M_{10}	54
11	SOH	M_{11}	2
12	››	M_{12}	187

mendekripsikan chiperteks dari B dengan melakukan perhitungan dengan rumus sebagai berikut :

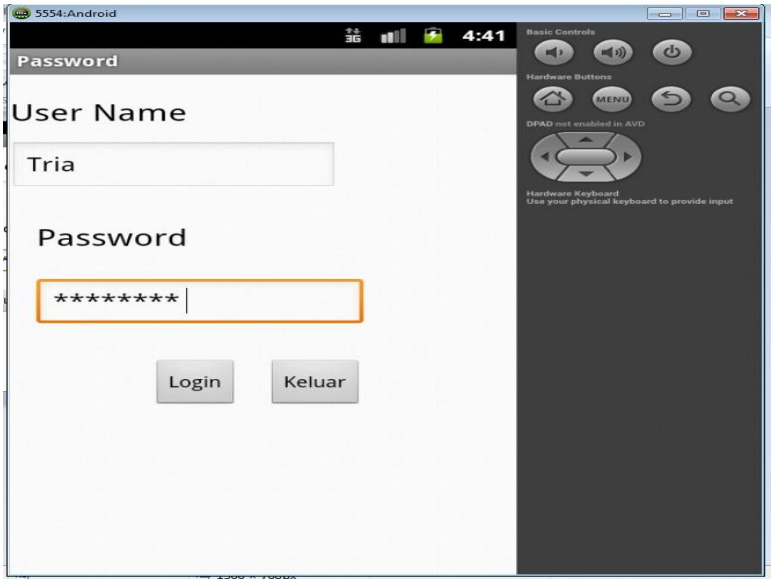
$$cn \equiv bi.ai^{p-1-x} \ mod \ 257$$
$$c1 \equiv 223.34^{257-1-11} \ mod \ 257$$
$$c1 \equiv 204.34^{245} \ mod \ 257$$
$$\mathbf{c1 \equiv 84}$$
$$c2 \equiv 147.15^{257-1-11} \ mod \ 257$$
$$c2 \equiv 147.15^{245} \ mod \ 257$$
$$\mathbf{c2 \equiv 82}$$
$$c3 \equiv 162.197^{257-1-11} \ mod \ 257$$
$$c3 \equiv 162.197^{245} \ mod \ 257$$
$$\mathbf{c3 \equiv 73}$$
$$c4 \equiv 167.68^{257-1-11} \ mod \ 257$$
$$c4 \equiv 167.68^{245} \ mod \ 257$$
$$\mathbf{c4 \equiv 65}$$
$$c5 \equiv 54.120^{257-1-11} \ mod \ 257$$
$$c5 \equiv 54.120^{245} \ mod \ 257$$
$$\mathbf{c5 \equiv 78}$$
$$c6 \equiv 187.2^{257-1-11} \ mod \ 257$$
$$c6 \equiv 187.2^{245} \ mod \ 257$$
$$\mathbf{c6 \equiv 73}$$

Setelah mendapatkan nilai mn, masing-masing nilai m hasil dekripsi menjadi kode ASCII diubah kembali menjadi karakter. Dengan hasil sebagai berikut :

Tabel 3 Konversi plainteks ASCII ke karakter

Plainteks Kode ASCII	Karakter
84	T
82	R
73	I
65	A
78	N
73	I

Berikut adalah hasil implementasi dari aplikasi pengamanan pesan.



Gambar 1. Form Login

Gambar 2 Form Menu Utama

KESIMPULAN

Adapun yang menjadi kesimpulan dari penelitian ini adalah:

1. Aplikasi chatting yang dirancang dengan menggunakan software Eclipse Galileo sebagai editor, software Development Kit (SDK) sebagai platform
2. Algoritma ELGamal diterapkan dengan menginput plainteks dan memasukan kunci rahasia yang sudah ditetapkan oleh client dan server
3. Aplikasi yang telah dijalankan dipindahkan ke handphone android dengan format .apk.

DAFTAR PUSTAKA

[1] M. Simanjuntak, T. Pasaribu, and S. Rahmadilla, "Implementasi Algoritma Merkle Hellman untuk Keamanan Database," *MEANS (Media Inf. Anal. dan Sist.*, vol. 4, no. 1, pp. 46–50, 2019.
[2] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.
[3] T. Limbong, "Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab," *no. Sept.*, vol. 2017, 2015.
[4] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
[5] T. Arianti and B. Nadeak, "Perancangan Aplikasi Pembelajaran Kriptografi Algoritma GOST dengan Menggunakan Metode Computer Based Instruction," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu*

Komputer), vol. 1, no. 1, pp. 40–46, 2019.
[6] W. Dwiono and T. Hartanto, "Penerapan Algoritma Kriptografi ElGamal Untuk Pengaman File Citra," *J. EECCIS*, vol. 4, no. 1, pp. 8–11, 2010.
[7] H. Aditya, I. N. Farida, and R. A. Ramadhani, "Heru Aditya Penerapan Algoritma Elgamal dan SSL Pada Aplikasi Group Chat," *Gener. J.*, vol. 2, no. 1, p. 48, 2018, doi: 10.29407/gj.v2i1.12052.
[8] Triase, "Kriptografi elgamal menggunakan metode mersenne," *Integritas*, vol. 1, no. 4, pp. 1–2, 2015.